State of Kansas

Default Information Technology Security Requirements

PUBLISHED BY:

KANSAS INFORMATION TECHNOLOGY EXECUTIVE COUNCIL

MARCH 2006

Table of Contents

1. Introduction

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and wider variety of threats and vulnerabilities. The purpose of this document is to provide the *Default Information Technology Security Requirements* that are referred to in the Information Technology Policy 7230- Information Technology Enterprise Security Policy. If an Agency does not have a security policy then this document becomes the Agencies Security Policy. It applies to all Agency's computing and network environments. If there is a conflict between this document and another Agency policy document, the document with the more stringent control will take precedence.

The foundations of this policy are the security concepts of:

- Business need-to-know
- Least privilege
- Separation of duties
- Risk Management
- Accountability, and
- Auditability.

This document should be used as a template for a starting point in the developing of an Agency Security Policy. State agencies should review this document, along with the Kansas State Technical Architecture, and use them to create individual agency security policies that meet the specific needs of their environment.

Agencies are also cautioned that documents of this type are considered Open Records. Therefore, sensitive security related details should be maintained in a separate, non-public security procedure manual.

1.1 General Policy Statement

Information is a State of Kansas asset requiring protection commensurate with its value. Measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional, as well as to assure its authenticity, integrity, availability, and confidentiality.

1.2 Scope

The controls in this document are the minimum requirements for providing a secure environment for developing, implementing, and maintaining systems in the Agency.

This policy applies to all Agency employees, agents, associates, representatives, interns, contractors, temporary employees, auditors, assignees, or other designates, or vendors involved in the development, implementation, and maintenance of information systems.

1.3 Compliance

All Agency employees, agents, associates, representatives, interns, contractors, temporary employees, assignees, or other designates, and vendors are responsible for understanding and complying with all Agency Security Policies. This would include building and configuring systems in accordance with these policies. Non-compliant situations will be brought to the attention of management for appropriate action. Employees who violate these policies may receive disciplinary action as specified in Agency conduct and disciplinary procedures. Depending on the severity, the Agency authority may remove the employee's network connectivity, and the

employee may be subject to Agency disciplinary actions, up to and including immediate dismissal and violators may be subject to criminal prosecution.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships, and alliances, must be monitored and reviewed to ensure compliance with Agency policies, and all applicable state and federal policies. This should be accomplished through contractual commitments with provisions to permit internal and external auditing and monitoring to ensure compliance.

All necessary exceptions to this policy must be clearly documented and approved by the Agency Head or designee when this document is used as the Agency's Security Policy.

Agencies must submit a copy of its Security Policy to the Chief State Security Officer on an annual basis or whenever significant are made to the Policy.

1.4 Document Changes and Feedback

Agency Security Policies must be reviewed annually by the Agency and updated as necessary for changes. If there is a major change in security requirements during the year, an addendum will be issued and communicated to Agency managers for dissemination to appropriate personnel. Discrepancies from the Agency's current policy should therefore be reported as soon as possible to the Agency security staff for review and inclusion in the next version or addendum.

1.5 Acceptable Use Policy

The Agency must have an Acceptable Use Policy for Agency provided Information Technology Resources. All employees must be required to annually read it, and sign an Employee Consent Form indicating that they have read, understand and consent to the Agency's Acceptable Use Policy. This form will be stored in the employee's personnel file.

1.6 Confidentiality Provisions

If the Agency uses any type of confidential information (such as IRS data), the Agency must develop a Confidentiality Policy and an associated Confidentiality Oath. This Policy should cover all confidential information whether state or federal and enumerate the civil and criminal sanctions against unauthorized disclosure.

All employees must be required to read the Confidentiality Policy annually and sign the Confidentiality Oath, which will be stored in the employee's personnel file.

1.7 Card Keys

For Agencies who use the Department of Facilities Management installed a Card Key System, a Policy and Procedure document should be created to define the Agency's rules for Card Key Management.

2. Organizational Roles & Responsibilities

Information security requires the active support and ongoing participation of individuals from all departments and management levels of the organization. It requires support from the executive level and compliance from everyone.

The following are suggestions for specific roles and responsibilities both at the management and staff level. When roles and responsibilities are assigned, the "separation of duties" concept must be taken into consideration to ensure the Agency's assets are adequately protected.

2.1 Agency Head

The Agency Head is ultimately responsible for carrying out the Security Policies in the Agency and for their development and implementation.

2.2 Data Owners

Data owners are the person(s) responsible for collecting, ensuring protection of, and authorizing access to data. Data owners should assess the risks to the integrity, confidentiality, and availability of information systems data and resources.

The owner is responsible and authorized to:

- approve all access to resources under his or her responsibility
- judge the asset's value and determine the sensitivity of the data
- ensure compliance with applicable controls through regular review of data classification and authorized access.

2.3 Custodians

Custodians are those person(s) delegated the responsibility of managing, handling or protecting access to data by the Data Owner.

Custodians are responsible for the safety and integrity of data in their custody. The custodian has responsibility to:

- implement the controls specified by the data owner
- provide safeguards for information resources
- administer access to the information resources and make provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources or inadvertent exposure due to mistake or loss of information.

2.4 Users

Users are all people who use State information assets for business purposes. This means that the user must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

Users have the responsibility to:

- use the resource only for the purposes specified by its owner
- comply with controls established by the owner or public law
- prevent disclosure of sensitive information
- comply with the Agency Acceptable Use Policy (see section 1.5)
- comply with the Agency Confidentiality Agreement (see section 1.6)
- receive Security Awareness training on an annual basis.

2.5 Security Administration

The Agency will appoint a Security Officer or designate someone within their organization with the responsibility of overseeing the information technology security functions of the department or Agency, including security administration.

The security administration function provides administration for user access to systems. These responsibilities include, but may not be limited to:

- authentication (add, change, delete) services to provide users with user ids and passwords
- authorization (add, change, delete) services to provide user access to applications
- generation and distribution of reports for monitoring access and potential security breaches
- management of the development and maintenance of Agency security policies and procedures deployment of mandatory annual Security Awareness training for all employees.

2.6 System Administration

The system administration function monitors performance, provides problem determination, production support, and performs system back-ups. Security responsibilities can include, but may not be limited to, ensuring that:

- only authorized software is installed via authorized means
- approved security procedures are followed and procedures are established where necessary
- systems are recovered in a secure manner
- ad hoc system reviews are performed to identify unusual activity
- systems are installed and operated using no less than the security controls provided by the vendor and using any security controls specified in the Agency's applicable security policies
- the security administration function is notified of changes to software that might impact system security features before installation of those changes and,
- procedures for software license validation and virus testing have been followed.

2.7 Database Administration

The database administration (DBA) function at the Agency has responsibility for all Agency owned databases. DBAs are responsible for the development, maintenance, and integrity of these databases unless otherwise specified by the database owner. Security responsibilities include, but may not be limited to:

- designing, developing, organizing, managing, and controlling the database in accordance with security policies
- providing the security administration function with the necessary information to maintain user ids and privileges and
- recovering databases in a secure manner when damaged or compromised.

2.8 Computer and Network Operations

The computer and networks operations and support functions are responsible for operating, supporting, and managing information systems and networks in accordance with the Agency Security Policies. Security responsibilities include, but may not be limited to:

- monitoring resources for signs of security violations
- ensuring systems and network architectures maximize security of those resources
- coordinating configuration with security administration to ensure all security policies are correctly enforced
- ensuring network security doesn't conflict with application security and,
- following specified escalation procedures for reporting security violations.

2.9 Application System Development

Application and system developers are responsible for ensuring that the systems developed, including purchased systems, are created according to the Agency Security Policies and any additional technical specifications that may apply.

2.10 Personnel Services

Working in conjunction with IT Management, Personnel Services' responsibilities include, but may not be limited to:

- ensuring that IT positions have job descriptions that accurately reflect appropriately segregated duties and responsibilities
- determining any necessary security clearances for individuals working with sensitive and/or confidential data
- conducting background checks as necessary for individuals in positions with sensitive job duties and responsibilities
- providing for appropriate division among several individuals for any highly secure functions
- establishing hiring, transfer, and termination procedures to promptly establish, modify, and close out security access
- documenting that all employees sign the Employee Consent Form for the Acceptable Use Policy and the Confidentiality Oath
- requiring that regularly scheduled vacations be taken
- promptly enforcing the Personal Conduct and Disciplinary Procedures for any significant security violations
- providing mandatory annual Security Awareness training for all employees and document attendance and maintain records.

2.11 Legislative or Internal Auditors

Auditors evaluate the compliance with the Security Policies through periodic examinations of information systems and applications, including verification that the appropriate management processes have been effectively applied. They are to be given necessary access to Agency premises, personnel, systems, and records to conduct their business.

2.12 Risk Management

The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The network will be continually expanding and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving. (see also National Institute of Standards and Technology: Risk Management Guide for Information Technology Systems, Pub. 800-30)

The Agency will develop an inventory of critical information assets. Each division within the Agency must prioritize its applications in the application priority list in the Agency contingency plan. The Agency IS management will identify and analyze threats to the critical information assets to determine the likelihood of their occurrence and their potential to harm these assets. Security policies and procedures will be evaluated and documented to reduce these risks to acceptable levels. (see also Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments, CMU/SEI-2005-TN-032, Carnegie Mellon University, September 2005)

The Agency IS management will annually update the State of Kansas Information Technology Security Self-Assessment in accordance with ITEC Policy 4310.

3. Vendor/Contractor Relationships

Allowing access to State of Kansas information to anyone outside the Agency may be necessary at times but this access must be carefully considered. There are occasions when vendors and contractors will require access to the Agency systems and the Agency must take precautions to protect all State of Kansas information as well as any Federal Tax Information it has.

All vendor/contractor contracts are handled through the Purchasing Office. The following are some considerations when working with vendors:

- Access should be restricted to specific IT data or resources.
- Specific language must be included in the contract to ensure compliance with the Agency security requirements.
- Where appropriate, Agency Confidentiality Agreements will be signed.
- Agency reserves the right to inspect vendor's security measures and pre-approve all sites/facilities.

4. Security Incident Reporting

There are several categories of information security incidents. Some examples are loss of service, human errors, computer fraud, viruses, network penetration, and loss of data or equipment. All suspected information security incidents must be reported as quickly as possible through the appropriate channels.

The responsibilities of the various parties are as follows:

- All employees, contractors and third party vendors should be required to immediately report suspected security breaches to their immediate supervisor.
- Employees, contractors and third party vendors should be advised that they should not, in any circumstances, attempt to prove a suspected weakness, without expressed prior authorization.
- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. Supervisors must notify the appropriate business area manager and the Agency Security Officer or designee
- Each Agency's d Chief Information Officer, or senior IT Manager, will investigate, research, resolve, and document the event. If the event the Agency determines the event is of enough significance and seriousness, it shall be reported to the Kansas Information Technology Security Officer.

See Appendix D for the Stages of Responding to Incidents.

5. Application/System Security Planning Process for Development or Modification

The Agency is required to submit an annual IT Management and Budget Plan in the fall of each year. Part of the plan lists detailed information on the new system proposals for the coming 3 years. As part of the process, these systems must have a Security Statement, which is a description of security features incorporated into the project.

Appropriate Information Security and Audit controls must be incorporated into all new systems. The ultimate responsibility for insuring appropriate levels of security and audibility lies with the application owner. In conjunction with the application developer, the owner must define the level of security based on the sensitivity and criticality of the data being processed.

IS Management must authorize all interconnections to others systems, and appropriate controls must be established and communicated to owners of the other systems.

The Agency will annually update the State of Kansas Information Technology Security Self-Assessment in accordance with ITEC Policy 4310.

During the course of the system development, or when new systems are acquired, the following areas of security will be addressed (Note that these are the same categories as on the Security Self-Assessment):

Management Controls
1. Risk Management
2. Review of Security Controls
3. Life Cycle
4. Authorizing Production

Operational Controls
5. Personnel Security
6. Physical and Environmental Protection
7. Production, Input/Output Controls
8. Contingency Planning
9. Hardware and System Software Maintenance
10. Data Integrity
11. Documentation
12. Security Awareness, Training, and Education
13. Incident Response Capability

Technical Controls
14. Identification and Authentication
15. Logical Access Controls
16. Audit Trails

In addition, for Web-enabled applications, the Web-enabled Security Questionnaire (Appendix E) will be completed.

To the extent that specific hours and costs of integrating security features into the project are determinable, these will be reported.

The Agency Chief Information Officer (CIO) and Security Officer (SO) or appropriate Agency Head designee should be contacted in the beginning phase of all system projects. Security should be considered at all stages of system development. The project manager must obtain sign-off by the owner and the CIO and SO or Agency Head designee before any system is approved. Final approval of the overall system, for

projects over $250,000., will be given through the approval process of the IT Plan by the Kansas Information Technology Office (KITO).

Agency programs and supporting computer applications frequently undergo modifications that may affect an existing security system. To ensure that security issues are considered when changes do occur, system documentation should address the impact modifications may have on the existing security system. Security procedures should ensure that the security system and its supporting documentation are periodically reviewed and, if need be, corrective action is planned for and implemented.

6. Testing Security Functions during System Development

Each new system being developed shall incorporate audit controls and testing of security. The ultimate responsibility for insuring that security and audibility have been tested lies with the application owner. The following security aspects will be performed during testing or when new systems are acquired:

- Include approved security requirements and specifications in the development baselines.
- Develop security test plans to test the specifications.
- Conduct and document tests of security in the configured components and in the integrated system.
- Prepare documentation of security controls and assign to the documentation the appropriate level of sensitivity.
- Conduct acceptance test and evaluation of system security prior to placing the system into production.
- Identify any security deficiencies promptly, correct them, and retest the system.
- Obtain appropriate signoff for security testing from the application owner.

The following procedures will be adhered to for testing systems:

- The test functions must be kept either physically or logically separated from production functions.
- Acceptance testing of programs will be performed by a test team independent of the programming staff.
- Members of the test team should be drawn from the specific business community who will use the modified programs.
- Test files separate from production data will be used for all testing.
- Change Control procedures must ensure that the appropriate manager has authorized all moves between test and production environments in writing.
- A naming standard should be in effect to distinguish between test jobs and production jobs, test data sets and production data sets.

7. Revision Management

Revision management is a critical security ingredient in systems development, testing and maintenance. The following policies must be followed:

- Only one version of the application programs will ever reside in production libraries.
- The persons writing or maintaining code must not be the same person(s) who migrate code to production libraries.
- Only authorized personnel, with appropriate security permissions, should apply program changes, catalog and copy newly updated programs to production libraries.
- Once an application has been placed in production, all program changes must be approved by IS management to insure the changes have been authorized, tested and documented.
- The software change procedures shall include written notification to the appropriate departments of the change.
- Change Control procedures must ensure that the appropriate manager has authorized all moves between test and production environments in writing.

- Program development personnel shall access production data and production program files only to resolve emergencies. The appropriate management shall log all such accesses.
- All programs shall be installed into production from the source code. That is, the appropriate change control staff will recompile the programs into the production libraries.
- Software that is downloaded from the Internet shall not be used for processing confidential or sensitive information, until such software is thoroughly researched and tested to ensure it does not contain malicious code.

8. Information Security

Protecting an Agency's information assets involves many issues and requires a systematic approach to ensure all aspects are considered and harmonized into an overall plan. The following major categories will need to be addressed:

- Authorized use and ownership of information resources
- Availability of critical data and systems
- Physical security
- User security
- Application security
- System security
- Data security
- Network security
- Security administration
- Social engineering/human factors

Policies for these major categories are as follows:

8.1 Authorized Use and Ownership of Information Resources

All information and telecommunication resources leased or owned by the Agency and all processing services billed to the Agency are only to be used to conduct State government business, except as otherwise provided by management directives.

A warning banner (similar to the one below) must display on the workstation when the user logs on:

Warning-Use of this system is Restricted
Access to this system is restricted to authorized persons having official business reasons to make such access. Use of Agency Information Technology Resources is subject to the Agency Acceptable Use Policy and Confidentiality Agreement. The Agency reserves the right to monitor, access, retrieve, read, and/or distribute, for official purposes, any information or communications sent or stored on IT resources, and it, in fact, does so as it determines necessary. Any violation of Agency policies and guidelines may result in disciplinary action, up to and including dismissal.

All computer software programs, applications, source code, object code, and documentation is Agency property and will be protected as such if developed either:

- by Agency employees in the course and scope of their employment or with the use of Agency equipment, materials, or other resources or
- by contract personnel acting under a contract with the Agency, unless the contract under which the software or documentation is developed specifically provides otherwise or
- with Agency funds.

All computer software programs, applications, and documentation purchased for the use of the Agency is Agency property and will be protected as such.

It is a violation of the Agency policy to copy proprietary software in violation of a licensing agreement. This includes downloading files from the Internet using peer-to-peer (P2P) software in violation of copyright laws.

The above policies are meant to be interpreted consistently with Information Technology Policy 8010- Ownership of Software Code and Related Intellectual Property. Policy 8010 states in part: "Unless explicitly covered in a contract executed by an authorized state official, all computer software and related intellectual property developed by State employees or (contract) personnel, or companies, on behalf of the State is the sole property of the State." Please refer to Policy 8010 for more information.

8.2 Availability of Critical Data & Systems

The State of Kansas, Executive Branch Chief Information Technology Officer requires agencies to have a Business Continuation Plan that includes the procedures necessary to assure the continuation of vital State operations in the event of a disaster. Each division within the Agency must identify and prioritize its processes in its continuation plan.

The Business Continuation Plan must outline the internal policies and procedures that are to be employed should a disaster occur. Preparation of the recovery strategies for all time-sensitive processes must be coordinated with the Agency's Business Continuation Manager. In the event of a disaster all time-sensitive services, systems and applications must be restored and available on a priority basis to maintain vital Agency operations.

Time-sensitive applications include those systems whose loss or unavailability is unacceptable to the citizen's of Kansas. The loss or unavailability of support services provided to these applications may adversely affect the continuation of vital programs and services or the fiscal or legal integrity of the Agency operations.

8.3 Physical Security

Physical Security involves the protection of the physical devices or hardware as well as controlling access to such hardware.

The following practices must be adopted in order to maintain adequate physical security within the Agency offices:

8.3.1 Access control measures

- All servers and other sensitive pieces of hardware should be kept in locked rooms.
- All hub rooms, communications rooms for telecommunications and wiring closets must be secured and kept locked at all times, unless personnel are working in such rooms.
- Secure storage areas for laptop computers should be available within Agency offices.
- Laptop computers that are used outside the office and that contain confidential information should have some means of protecting the data, such as encryption or maintaining the data on removable disks.
- Whenever an employee leaves the Agency for other employment the immediate supervisor must obtain the employee's building passes and card

keys. The supervisor must also notify Security Administration immediately upon an employee's separation.
- An Agency must have policies and procedures in place for locking doors after work hours.
- The home user of Agency equipment must ensure that unauthorized access to Agency resources is prevented.

Raised floor computer rooms must include the following control measures:
- Walls separating work areas on raised floors where the level of security is different on either side of the partition must extend and completely shut off the area between the raised floor and the permanent floor.
- An access card system will be used to control access to the room and will signal an alarm when unauthorized entry is attempted.
- Only persons whose work requires them to be in raised floor computer rooms on a day to day basis will be granted access cards to those areas.
- All visitors to computer room facilities must sign in on a log.
- Logs of all visitors to computer rooms will be maintained for a minimum of 1 year for audit purposes.
- Formal procedures must be established for the issuance and removal of card keys.
- Security Administration is responsible for processing requests for new cards, changes to existing cards and deletions of cards.

8.3.2 Fire Suppression Measures

- All Agency work areas must have hand-held fire extinguishers available in accordance with published fire prevention standards for public access buildings. A licensed extinguisher inspector must check these extinguishers on at least a yearly basis.
- Care must be taken to properly store flammable solutions or materials
- Fire doors are not to be propped open for any reason.
- All Agency employees will participate in regularly scheduled evacuation drills.

With regards to Raised Floor Computer Rooms:
- Low Flame spread materials are to be used wherever practical in the construction of computer rooms
- Dampers and Shutters are to be included in the heating and cooling subsystems of buildings housing computers that can be closed to slow the spread of fire.
- Detection equipment must be included in the construction of computer rooms that activate alarms at a centrally located console area. This equipment must be tested on a regular basis.
- Sprinkler systems in computer rooms must be of the "dry line" type to prevent accidental discharge of water on electronic equipment.
- If dry chemical type extinguishing systems, such as Halon, are used in computer rooms, these systems are to be checked by qualified technicians on at least a yearly basis.

8.3.3 Environmental Measures

With regards to Raised Floor Computer Rooms:

- Adequate air handling equipment must be installed to insure room temperatures consistent with computer equipment needs. Redundancy

should be included to accommodate times when primary equipment is down.
- The area below the raised floor must be thoroughly cleaned at least on a yearly basis to prevent circulation of harmful dust particles.
- Monitoring equipment must be installed to track temperature and humidity. This equipment must be capable of sounding an alarm should one of these environmental conditions exceed predetermined thresholds.

8.3.4 Electrical Power Measures

- Uninterrupted Power Supply (UPS) systems must be utilized to assure continuous power to systems deemed critical to Agency business.
- Surge protection equipment should be utilized to protect electronic equipment that might be sensitive to power fluctuations.
- Maintenance technicians working on or around electronic data processing equipment must wear static electricity eliminating bracelets.

8.4 User Security

User Security addresses the ability to ensure that the user accessing data and systems is in fact who they say they are, present the necessary credentialing information for access, and that they have access only to those resources to which they are authorized. Functions that are involved include identification, authentication, authorization, non-repudiation, and audit.

8.4.1 Identification

The Agency must require that all users accessing protected information systems are properly identified. Each user must be required to provide some unique identification (User Id, token, biometric) to provide a claimed identity to the system. No guest or anonymous accounts will be allowed.

User Ids must:

- be unique and identify only one individual user
- not be shared and group user-ids should not be permitted, except where required by specific applications or computer platforms
- have their privileges terminated when they become inactive or dormant after a certain period of inactivity
- use a standard format developed by the Agency across all platforms to ensure uniformity
- only be issued after Security Administration receives a properly authorized request, indicating type of access desired
- be immediately disabled when the user's employment is terminated or the user transfers to a position where access is no longer required. The immediate supervisor or manager should initiate removal notification
- be suspended after 3 unsuccessful log on attempts.

Passwords must be:

- individually owned
- kept confidential and not shared with other users
- changed whenever disclosure has occurred or may have occurred, and changed at least every 60 days

- changed significantly (i.e., not a minor variation of the current password)
- a minimum of seven characters and contain alphanumeric characters and where allowed include special characters

Passwords must not be:

- repeated for at least six cycles of change or a year
- repeating sequences of letters or numbers (e.g. rrr, 123123)
- names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names)
- the same as the user id
- words that can be found in a dictionary
- displayed during the entry process
- written down and displayed in an obvious place
- the same for all systems the user accesses
- stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.

The Agency CIO or senior IT Manager and the Security Officer or the Agency Head designee must approve all exceptions.

Vendor installed default passwords w must be changed immediately. If vendors require access to the system remotely for maintenance, they should be provided temporary passwords that are changed after they have concluded any maintenance.

Having and supplying the correct information authenticates an individual to the data processing system. Similarly, a computer, terminal, or other peripheral may be authenticated as an authorized device of a data processing system.

8.4.2 Authentication

The need for authentication is a response to the need to avoid or reduce the risk that the wrong person will access, use change, delete or otherwise improperly interact with valuable data or transactions
Authentication is the process and documentation required to validate a user's claim to who he/she is. Authentication can also be a process in which electronic devices validate who they are to one another. The strength of authentication can range from weak to strong. The selection of authentication strength should be based upon the level of risk consequence if security was breached

The Agency must require all users to be authenticated. Authentication should be based on something the individual knows (e.g. a password), something the individual possesses (e.g. a digital certificate, or smart card/smart token), or by something the individual is, (something which relies on measurable physical characteristics).

Systems must implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information they contain and process. When considering authentication techniques, first determine if the confidentiality and/or criticality of the information processed by the system requires stronger authentication than passwords alone. If so, then consider smart cards, smart tokens, digital certificates or biometrics.

8.4.3 Authorization

Once identified and authenticated, Users must only have access to those resources to which they are authorized.

Authorization involves the determination of the proper level of access for all users for all systems, based on need to know, specific job responsibilities, and sensitivity of the data. The following points identify attributes of an effective authorization system:

- The authorities to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information.
- Users shall be granted rights and privileges to available system resources only on a need-to-know, need-to-use basis. Users should be limited to the minimum rights and privileges to do their jobs.
- Individuals may be granted a specific combination of authorities.
- Data owners or their designees should review users' rights and privileges annually.
- Security administration should not require programmer intervention.
- Security administration activity should be recorded and reviewed and security violations should be detected and reported.
- There should not be any access available to programmers that is not provided through standard, approved connections. In other words, "backdoors" should not be permitted.
- Programmers responsible for development activities should not make changes to production application code without using the authorized change control procedures.
- Access rules or profiles should be established in a manner that restricts departmental employees from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.
- Procedures are enforced so that application programmers are prohibited from making unauthorized program changes.

8.4.4 Non-repudiation

Non-repudiation is the proof that a transaction is performed and is a requirement for web-based application transactions between two parties. If a party to a transaction or communication later denies it has ever happened, some mechanism must be in place to facilitate dispute resolution. Public Key Infrastructure (PKI) technology in conjunction with transaction audit logging may be used to provide the assurance that the information received has not been altered and that the reputed sender of the information is indeed who sent it. (Refer to 9.2 Public Key Infrastructure)

8.4.5 Audit Trails

Automated records should be maintained to enable reconstruction and/or review of transactions performed on systems by users. Audit trails should be protected in such a way that a user can not change them. They should be reviewed

regularly by individuals in a supervisory or security capacity, using automated tools where possible to review them.

Audit Trails for two other types of activities are also very important.

Security Administration Activities.

Access to security administration software must be restricted to personnel who have security administration duties. Audit trails must be maintained to provide accountability for all security administration activity. Software products used to administer security on all Agency systems must be able to record and report all security administration activity. Systems should also provide a means to recover current and historical information about security administration activities in the event of a system failure.

Security administration products and procedures must log all security violations. Resultant log files should be reviewed by security administrators and data owners to detect any unusual or inappropriate activity. In addition to checks against authorizations, particular attention should be paid to unusual times, frequency, and length of accesses, as well as irregularities that could indicate potential violations. Log data must be kept at minimum of 30 days.

The system must not disclose passwords through reporting functions.

Procedures must exist to maintain the integrity of access tables within security enforcement software.

Database and Other Logging.

Automated chronological or systematic records of changes to data are important in the reconstruction of previous versions of data in the event of corruption. These records are useful in establishing normal activity, identifying unusual activity, and in the assignment of responsibility for corrupted data.

A complete history of transactions will be maintained for each session involving access to confidential information to permit an audit of the system by tracing the activities of individuals through the system. The department's owner of data must determine how, where, and, the length of time that these transactions will be maintained.

In addition to system start-up and shutdown times, transaction histories should log the following information:

- update transactions
- date, time of activity
- user identification
- sign-on and sign-off activity and
- confidential display transactions.

DBA s' security actions should also be logged. Only designated personnel should have access to the transaction histories and to the results of any analyses.

Where confidential information involves the uses of Federal Tax information from the IRS, or any other data protected by Federal laws and regulations, appropriate audit trails must be maintained.

8.5 Application Security

Application Security concerns the built in security features of the application itself.

Application developers and owners should ensure that the security features of the application code are consistent with the overall security policies enumerated in this document.

Network access to an application containing confidential data, and data sharing between applications, shall be as authorized by the application owners and shall require a level of authentication commensurate with the level of risk determined during the risk assessment process.

The owner of applications containing non-critical or non-sensitive data should likewise establish criteria for access and user validation, particularly on systems authorized for public use.

8.6 System Security

System Security involves the analysis of the overall operating systems and software used to support the applications software. Whether the operating system is mainframe, server, or PC based, or a combination thereof, operating system technicians should:

- Ensure that research is done to identify security vulnerabilities.
- Maintain a log of investigations for these vulnerabilities for future reference.
- Maintain a system to become aware of, test and install vendor-supplied security upgrades and patches.
- Review and change vendor-supplied security parameters as required.
- Change shared system admin passwords when an employee with system administration responsibilities leaves the Agency.
- Utilize standard base configurations for operating systems on servers and workstations.
- “Harden” servers based on industry guidelines.
- Remove or disable any service not required.
- Test all upgrades or new releases of system software before deploying to production. Include analysis of any changes affecting security controls and training necessary to implement them.
- Acquire additional security software as needed to reside on the system to enable Agency to move from a reactive to a proactive environment.
- Install firewalls and monitor them.
- Install intrusion detection/prevention systems and monitor them for unauthorized access.
- Conduct periodic vulnerability scans and consider security audits by outside third parties to pinpoint the weaknesses of the system.

8.7 Data Security

Data security encompasses:

- protecting the data from unauthorized access:
- when stored on computer systems,
- when transmitted over public networks (see the Encryption section)
- protecting the loss of data through:
- mechanical /electrical failure,
- viruses (see the Virus Protection section under Issue Specific Policies),
- or any other disaster.

Data backup, archiving and off-site storage procedures are all important to mitigate the risk of losing data. Proper data disposal procedures are important as well to protect confidential data from being accessed by unauthorized personnel.

8.7.1 Data Access

Data is an important asset of the Agency and shall be protected by all users by strict adherence to the following policies:

- Guest or anonymous accounts will not be allowed to access Agency data.
- Agency naming conventions for data sets/files shall be followed to ensure uniformity and to facilitate security access control.
- Agency employees shall only access Agency data that is necessary to perform their job responsibilities.
- Agency employees shall safeguard all data labeled as confidential per Agency Policy.
- Agency employees shall erase white boards containing confidential information immediately after completion of use.
- Agency employees shall remove confidential information from printers or FAX machines immediately.
- Agency employees shall remove and secure confidential information from their work area when they leave.
- Agency employees shall not make any unauthorized additions, changes, or deletions to any Agency data in any form. (e.g. spreadsheet, data set, database, etc.) Agency employees will defer to the data owner regarding any decisions as to the disposition of said data.
- Agency employees will use only authorized software and business applications to change, manage, or replicate Agency production data. This normal business activity allows for security and transaction logging as designed in Agency production systems.

8.7.2 Data Backups

Regularly scheduled backups are an integral part of Data Security. The ultimate responsibility for establishing backup procedures lies with the data owner. Backups of mission critical data must be kept offsite, in a secure location, to insure recoverability in the event of a natural disaster. The security of backup media must be ensured at all times during the transfer to the offsite storage location. If outside couriers are used, the Agency Confidentiality Agreement must be signed.
Depending on individual circumstances, backups can be any of the following:

- Complete file copies
- Incremental backup copies which are copies of the changes since the last full backup in conjunction with full backups
- Database recovery logs which track database activity since the last full backup.

Recovery procedures must be documented and tested on a regular basis. All types of data should be included in backup procedures including but not limited to software program libraries, databases, Job Control libraries and electronic forms of documentation.

8.7.3 Data Disposal

The Agency requires that all users properly dispose of confidential data, regardless of the medium it is stored on, upon completion of the use of such data. Federal data will be disposed of in accordance with applicable Federal regulations.

8.8 Network Security

There are two types of access: trusted and un-trusted. Trusted access refers to access between State controlled nodes, systems, or networks. Un-trusted access refers to access between non-state controlled nodes, systems, or networks and state controlled nodes, systems, or networks.

In addition to the types of access, there needs to be considerations for public vs. private networks. Public networks are defined as those accessible to the general public, such as: the Internet, telephone lines, satellite links and wireless or cellular communications. Public networks are considered un-trusted therefore, all restrictions as applied to un-trusted will be applied to public. The Statewide KANWIN network is open and un-trusted. Private networks are defined as networks not available to the general public such as any Agency Local Area Network or Agency VPN. Private networks may only be considered trusted if the network is controlled from end to end by the Agency.

8.8.1 General Network Controls

Network resources participating in the access of confidential information shall assume the confidentiality level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.
All network components under Agency control must be identifiable and restricted to their intended use. Following are some guidelines:

- Terminal software locking options will be enabled on each terminal so that access can be controlled by locking the terminal while it is unattended.
- All line junction points (cable and line facilities) should be secured and located in secure areas.
- Control units, concentrators, multiplexers, switches, hubs and front-end processors will be protected from unauthorized physical access.
- Procedures will be implemented which ensure that access to security data or mission critical information is not dependent on any one individual. There should be more than one person with authorized access.
- Some types of network protocol analyzers and test equipment are capable of monitoring (and some, of altering) data passed over the network. Use of such equipment will be tightly controlled since it can emulate terminals, monitor and modify sensitive information, or contaminate both encrypted and unencrypted data.
- DISC is responsible to maintain up-to-date diagrams showing all major network components, to maintain an inventory of all network connections, and ensure that all unneeded connections are disabled. The Agency is responsible for its own network diagrams and collaborates with DISC as necessary.
- Default passwords on network hardware such as routers and switches should be changed immediately after the hardware is installed.
- The Agency must maintain a list of all approved dial access modems. The BIS should establish a procedure that periodically checks for any unapproved modems that have been added to the network.

- Each Agency must periodically monitor sharing and trusting relationships to ensure they are still valid.
- One, or more, persons in each Agency should be assigned the responsibility of (1) monitoring security updates that apply to the Agency's software, and (2) keeping security patches current.
- Consider the use of automated software to ensure that any device connecting to the network has the current level of security patches and anti-virus installed. Otherwise quarantine the device and update it first.
- Consider the use of in-house password cracking software.
- An Audit of network security should be conducted annually by DISC and Agency.
- An independent audit of network security by an outside third party should be considered on a periodic basis.

8.8.2 Distributed Network Access Security

Agency owned or leased network facilities and host systems are Agency assets. Their use should be restricted to authorized users and purposes. Where public users are authorized access to networks or host systems, these public users must be clearly identifiable and restricted to only services approved for public functions. Agency employees who have not been assigned a user id and means of authenticating their identity to the system are not distinguishable from public users and should not be afforded broader access.

The Agency BIS shall prescribe sufficient controls to ensure that access to distributed information resources served by distributed networks is restricted to authorized users and uses only. These controls shall selectively limit services based on:

- user identification and authentication (e.g., password, smart card/token) or,
- designation of other users, including the public where authorized (e.g., vendor access through dial-up or public switched networks), for the duration of a session or,
- physical access controls.

Guidelines for distributed network access:

- For distributed processing systems and local area networks, authorization at network entry shall be made on the basis of valid user identification (e.g., user id) and authentication (e.g., password, smart card/token).
- The host security management program shall maintain current user application activity authorizations through which each request must pass before a connection is made or a session is initiated.
- Unauthorized attempts (successful or otherwise) to access or modify data through a communication network should be promptly investigated.
- If unauthorized access or modification of data occurs, the Agency should promptly review its existing security system, including its internal policies and procedures. Appropriate corrective actions should be planned for, established, and reviewed by the Agency IS Bureau to minimize or eliminate the possibility of reoccurrence. Employees may need to be reminded of existing or revised procedures.

8.8.3 Network connectivity and Monitoring Controls

	CONTROL NAME	CONTROL STANDARD
1.	Connections	No communication modem, router, gateway or other network device or software may be connected to the State KANWIN network without approval from the DISC, Bureau of Telecommunications. All communications design architectures, connecting to the State network, must also be reviewed and approved by the DISC, Bureau of Telecommunications.
2.	Addressing	Network names and addresses should be coordinated by a central addressing authority.
3.	System and Node Authentication	Each system and node in a network must authenticate each accessing user, process, or other entity. This may be either through individual logon or by means of a single sign-on to a strongly authenticated state controlled security server. Connection paths, terminal addresses, node addresses or other identifiers do not constitute an acceptable means of user authentication.
4.	Trusted Node Authentication	The use of trusted nodes requires that the owners of all participating nodes agree to the adequacy of the controls for authentication of users of those nodes. Participating nodes must also authenticate the identities of other nodes. Connection paths, terminal addresses, node addresses or other node identifiers do not, by themselves, constitute an acceptable means of node authentication. Only state owned, operated, and controlled nodes located in restricted facilities may be trusted nodes.
5.	Network Diagnostic and Monitoring Tools	Possession, distribution or use of network diagnostic, monitoring, and scanning tools such as LAN analyzer and attack scanners (both hardware and software) is limited to designated and authorized personnel in accordance with their job responsibilities. This includes anything that can replicate the functions of such tools. Unauthorized possession, use, or distribution of such tools or functions is prohibited and may be grounds for immediate dismissal. Attack scanners should not be used outside the Department of Administration unless prior notice and authorization is granted in writing by the targeted agency.
6.	IP Address Classification	IP addresses for firewalls and other security servers are information intended solely for use within DISC and Agency and limited to those with business need-to-know. IP addresses will not be included in materials and planning documentation that will be released externally out of Agency BIS except to BOT/DISC.

8.8.4 Firewalls

The following are the Agency policies for firewalls:

- A firewall shall be placed between the Agency's network and the Internet/KANWIN to prevent untrusted networks from accessing the Agency network.
- All users who require access to Internet services must do so by using Agency-approved software and Internet gateways.
- Users must not circumvent the firewall by using dial-out modems or network tunneling software to connect to the Internet.
- The firewall will protect against address spoofing. The firewall shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.
- Anonymous FTP into the Agency's Network will not be allowed.
- The firewall must be configured to be the only host address that is visible to the outside network, or handle NAT for hosts which need unique addresses, requiring all connections to and from the internal network to go through the firewall.
- The firewall will enforce service rules (e.g. for http, telnet, ftp) in order to hide the identity of all Agency sub-networks and/or their users (i.e., private networks). All external to internal communications should go through the firewall rulebase. These rules will take external requests, examine them, and forward legitimate requests to the internal host that provides the appropriate service.
- When a service is required that is not supported by a rule, the service shall be denied until the service and rule can be evaluated and/or added to the firewall.
- The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.

8.8.5 System Identification Screens

Agency system identification screens should include the following warning statements:

- Unauthorized Use is Prohibited
- Usage May be Subject to Security Testing and Monitoring and
- Abuse is subject to criminal prosecution.
- Users have no expectation of privacy

Guidelines for system identification screens:

- The system identification screen should be implemented so a user cannot bypass it.
- The system identification screen should remain on display for a sufficient amount of time for the message to be read.
- If the system cannot display an identification screen with an appropriate warning message, the message should be included on a printed label affixed to each video display terminal.

- Identification screens must be approved by the Agency Security Officer or Agency Head designee.

8.8.6 Intrusion Detection/Prevention System (IDS/IPS)

The Agency shall maintain an appropriate Intrusion Detection/Prevention System (IDS/IPS). At a minimum, the IDS shall consist of at least 1 network sensor and multiple server sensors to protect those servers that host web applications.

Reports shall be generated daily and be available for review by the Security Officer or Agency Head designee.

8.9 Security Administration

Security Administration involves the administration of the overall security plan. Please refer to Section 2.5.

8.10 Social Engineering/Human Factors

Social Engineering/Human Factors are concerned with the techniques that employ the use of deceptive practices aimed at individual employees. Social engineers try to get employees to reveal Agency information they should not and then use that information to gain access to Agency systems. All computer networks and applications are susceptible to compromise by malicious or unauthorized persons. Employees should:

- Be aware they can be used as a resource to enable illegitimate access to systems or networks.
- Know what information should remain confidential and exercise caution to prevent the release of sensitive details to unauthorized sources.
- Clear their work areas of any confidential information when they are not present
- Always know the identity of whom is requesting the information and why they need to know it.
- Not share user ids with anyone, unless they know the requester is a Agency IS staff member and has a legitimate need to know.
- Never share passwords with anyone.
- Encourage vendors, outside technical support or contractors to contact Agency IS staff support for information pertaining to the network or information access.
- Inform their supervisor if anyone tries to obtain information they should not.

9. Data Encryption & Key Management

9.1 Data Encryption

Data encryption techniques are used to control access to information, protect the integrity of transactions, disguise data during transmission, and authenticate the users and devices of an information processing system.

Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. Readable text is converted to unreadable text, called cipher text, based on a

security key provided by the owner of the information. Anyone examining an encrypted file would see a string of unrelated characters or symbols. The encryption process can be reversed or decrypted only by someone who has the security key.

Encryption techniques can be divided into two general categories, symmetric or private key techniques and asymmetric or public key techniques. In private key encryption, the receiver of a message uses the same key to decrypt the message as the sender used to encrypt the message. Public key encryption provides both the sender and receiver with two keys, one private and one public. Private keys are the secret of their users, while public keys are openly available via a directory. When public key encryption is used, the sender encrypts the message in the public key of the intended receiver. Upon reception, the message is decrypted with the receiver's private key. Public key encryption technology simplifies the processes of key distribution and implementation of authentication functions.

9.2 Public Key Infrastructure

The State of Kansas has implemented a Public Key Infrastructure (PKI). PKI is the architecture, organization, techniques, practices and procedures that collectively support the implementation and operation of a certificate-based, public key cryptography system. (see also Kansas Certificate Policy, XXXX and Kansas Administrative Regulations 74-41-1 through 74-41-33).

A signing certificate, or key, is provided to a user to be used as a signature attached to documents, e-mail etc. The certificate is provided by the certificate authority (CA). Verisign is the CA for the state of Kansas through a contract administered by the Secretary of State. Requests for certificates are performed by Registration Authorities (RA). The RA for Kansas digital certificates is the Information Network of Kansas. RAs are required to sign agreements and be subject to audits by the Secretary of State and maintain all records surrounding the authentication of the requestor's identity.

Similarly, the RA takes the necessary steps to confirm a user's identity before issuing a signed certificate to the user. The user can then attach this certificate to any assurance to the recipient that the information came from the person that signed it. This serves as legal non-repudiation.

The user should protect this certificate since it is his legal signature, if it is in some way compromised this should be reported to the CA administrator immediately so that it can be revoked.

The State of Kansas Statewide Technical Architecture outlines the current & evolving encryption standards. This document should be reviewed before any standard is adopted.

9.3 Encryption Services

The table below contains some of the security services that may use encryption, a definition of the service, and encryption methodologies for that service.

SECURITY SERVICE	DEFINITION OF SECURITY SERVICE	ENCRYPTION METHODOLOGY
Confidentiality Protection	Protection from revealing information to unauthorized entities or individuals.	Encryption via VPN, PGP, and SSL

Integrity Protection	Preventing data from being modified or manipulated from its original state. In some cases, only integrity protection may be required, then confidentiality protection would not be required.	Checksums VPN
Non-repudiation Protection	The ability to demonstrate to a third party that the originator of a transaction did, in fact, originate that transaction and that the message was not modified.	PKI

9.4 Guidelines for Data Encryption

In making the determination to use data and file encryption, the following risks should be considered:

- loss of State funds
- violation of individual expectations of privacy
- violation of state or federal law
- civil liability on the part of Agency
- compromise of Agency legal or investigative efforts
- loss of business opportunities for affected persons and
- undue advantage to any person in Agency competitive business relations.
- Interception of unencrypted information may not be readily detectable. It should be assumed that unencrypted information is available to any intruder.
- When encrypted data is transferred between organizations, the respective Information Resource Managers should devise a mutually agreeable procedure for secure key management. In the case of conflict, the data owner should establish the criteria.
- Keys should be communicated separately from the encrypted information, preferably through different channels.
- Passwords and dial-up terminal identifiers should be encrypted during transmission and in storage. They should be encrypted during session logon if the information to be exchanged requires encryption.
- Encryption and decryption devices should be located as near the using devices (connected terminals and processors) as possible to minimize the need for other safeguards on the unencrypted segments of the link.
- Sensitive or critical information should be stored in encrypted form if physical controls are not sufficient. Volumes or files where all sensitive information is encrypted may be controlled as though the information is not sensitive as long as encryption keys are appropriately controlled.
- Security through encryption may be enhanced by requiring that two trusted individuals control the key each having custody of half the key.

- The need for encryption should be determined by the level of liability in the event of disclosure risk of the information and the location of the information.

9.5 Key Management

The functions associated with generating, distributing, storing, protecting, and destroying authentication and data encryption keys are collectively referred to as key management. Without adopting internal policies and procedures that address key management issues, an agency risks serious security problems. Specifically:

- an unauthorized individual possessing the key and having access to encrypted data might have access to confidential or sensitive information
- losing the key will render the agency unable to read or process encrypted data and,
- the agency cannot guarantee the security of its information.
- transactions can be reputed

Key management functions should be designed to protect authentication and data encryption keys and associated materials from unauthorized disclosure, substitution, insertion, deletion, and recording. Unauthorized attempts to access key management information should be detectable and unsuccessful.

10. Personal Computers and Agency Equipment

The Agency has issued an Acceptable Use Policy for Agency provided Information Technology Resources. These resources include, but are not necessarily limited to software, hardware, fax machines, pagers, cell phones, computer printers, E-mail, Internet, and voice mail.

Inappropriate use of the Agency's equipment may subject the employee to disciplinary action up to and including termination of employment.

10.1 Practices

10.1.1 Physical Security

The Acceptable Use Policy covers all forms of usage of these resources, whether used at work, at home, or in other locations. The Agency attempts to secure all computer resources used in the work environment and to restrict the access/entry of personnel to only authorized individuals.

Employees should notify their management immediately if they detect any Agency equipment is stolen or lost, or if they notice any unauthorized use or attempted misuse of Agency equipment.

Employees who use Agency provided resources at home or other locations should:

- maintain these resources along with any other communications equipment and circuits under the same guidelines as equipment located in a work environment
- be responsible for assuring that no unauthorized access is permitted
- not leave portable equipment unattended and lock them up when they are not in use
- take special care with portable devices when in public places to avoid loss.

When computer equipment is disposed of or de-installed and staged for surplus property, Agency procedures must be followed. These include the use of

software to overwrite the hard drive a minimum of 7 times, or the degaussing of and physical destruction of media containing Agency confidential or FTI data. Refer to the Agency Security Procedures for more information.

10.1.2 User Security

All users of Agency equipment should:

- protect their personal authenticators (passwords, PINS, smart cards, tokens, etc.) so others cannot use them
- change their passwords regularly in accordance with the Agency Policies
- place computer monitors in public areas to restrict unauthorized viewing
- not leave their workstation unattended while logged on without "locking" the workstation by pressing Ctrl-Alt-Del and then Lock Workstation.
- not attach any equipment to the Agency network without prior approval of the Agency IS management. This includes such equipment as Personal Digital Assistants (PDAs), and USB storage devices.

10.1.3 Application Security

Employees should:

- use only Agency-approved software that is owned or properly licensed the Agency
- be familiar with the various software applications they utilize and use them under the provisions of the Acceptable Use Policy
- promptly report any applications not operating correctly to their management

10.1.4 System Security

The proper installation of PC system software is the responsibility of the Agency. Employees should report any suspected malfunctions to their supervisor or Help Desk if applicable.

10.1.5 Data Security

Data Security encompasses both physically protecting the data from unauthorized access, as well as protecting it from loss. It is especially important to protect confidential data.

The Agency should issue a Policy regarding the inspection and disclosure of confidential information. All employees are required to read the Policy and sign the Confidentiality Oath. This Policy covers all confidential information whether state or federal and enumerates the civil and criminal sanctions against unauthorized disclosure.

Employees should take the following precautions:

- backup your "mission critical" files routinely
- know the level of sensitivity of the information that you are responsible for and with which you work
- erase white boards containing confidential information

- remove confidential information from printers or facsimile machines immediately
- remove and secure confidential information from your workspace
- use software access controls and encryption software on portable computers containing confidential information
- do not discuss or transmit confidential information on unencrypted cordless telephones, cellular phones or wireless modems because conversations can be easily intercepted and monitored
- never discuss or transmit confidential information without explicit authorization
- dispose of confidential data according to the Agency Policies.

10.1.6 Network Security

Direct dial-in to modems on the Agency LANs is not allowed without explicit approval of the CIO or the Agency Head designee. The use of software that permits a user to access Agency resources from home or when traveling away from the office should be managed closely to avoid compromising security policies. The use of software similar to PC Anywhere, or Carbon Copy, that make it easy for remote access terminals to function exactly as they would in the office should be avoided. It is the responsibility of the CIO or the Agency Head designee to assure that this type of software is not used without the proper review and management.

Distribution or use of network diagnostic, monitoring, scanning tools or hardware/software attack scanners is limited to designated and authorized personnel. If you distribute or use these tools without authorization, it can result in our immediate termination.

Do not answer any questions about the network, or how to access data on the network without knowing the person asking the questions. Answers to questions about the network and it's inter-working shall only be provided on a need to know basis.

10.1.7 Social Engineering/Human Factors

Social Engineering/Human Factors are concerned with the techniques that employ the use of deceptive practices aimed at individual users or employees.

Consequently employees should:

- Know the level of sensitivity of the information that you are responsible for and with which you work.
- Not disclose information to unauthorized persons.
- Always verify the identity and the need-to-know of anyone requesting information.
- Notify your management of unauthorized attempts to obtain information.

11. Issue-Specific Policies

11.1 Use of Federal Tax Information from the IRS

An Agency that receives Federal Tax Information (FTI) from the IRS must safeguard the FTI in accordance with IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies.* The requirements are in Appendix C: Requirements for Use of Federal Tax Information from the IRS.

11.2 Internet and E-Mail Access

11.2.1 Security

Do we want to include something here about the use of email services such as Hotmail?

Access to and from the Internet and through the e-mail system represents potentially significant security exposures for the Agency and the State of Kansas network. The following are the minimum controls required to establish an Internet or e-mail connection using Agency computing or networking resources. It applies to all individuals who use the Internet and/or e-mail with Agency resources as well as those who represent the Agency.

Users of Agency systems may not use State of Kansas facilities and connections to make unauthorized connections to, break in to, or knowingly, adversely affect the performance of other computer systems on the network. Access to other computer systems via the Internet does not convey the right to use or connect to these computer systems. This right only comes from proper authorization by the owners of those computer systems. Individuals must not "test the doors" or "probe" security mechanisms at either Agency or other Internet sites unless they have first obtained permission from the Agency CIO and Security Officer or the Agency Head designee.

Users of Agency systems are required to use all available methods to prevent unauthorized connections to State of Kansas networks. This includes taking such precautions as enabling approved virus protection software when connected to the Internet or receiving e-mails. This also includes prohibiting unauthorized persons from accessing State of Kansas systems through the user's logon or password, using password protected screen savers when the work area is unsupervised and taking any other prudent security precautions.

Agency confidential information must not be sent over the Internet or through e-mail unless it has first been encrypted by a Agency approved encryption method.

If a user suspects that sensitive Agency information has been lost or intercepted by unauthorized parties, the user is required to notify the Agency CIO and Security Officer or the Agency Head designee immediately.

The Agency will maintain a security statement accessible off of the home page on the Agency web site.

11.2.2 Privacy

The Agency maintains an electronic-mail (e-mail) system and Internet access to conduct State of Kansas business. This system, including the equipment and the data stored on the equipment, is at all times, the property of the State of Kansas.

The Agency cannot guarantee the privacy of electronic communications because electronic communications are not private by nature, and are inherently insecure. Employees should have no expectation of privacy when using e-mail systems or the Internet.

Even though passwords appear to provide confidentiality, privacy of messages cannot be assumed. This means that e-mail and Internet transmissions can be read, altered, or deleted by unknown parties without the knowledge or permission of the user who composed, sent, or received the message or its attachments(s). In addition, note that even when e-mail messages or Internet files are deleted or erased, it is still possible to recreate the original message or file.

Agency employees shall not leave phone messages, send e-mail messages, or create files that would embarrass them or the Agency if the contents were made public. Agency employees shall respect the privacy of others and not use any equipment (whether belonging to the Agency or to them) inappropriately. Examples of personal equipment include, but are not limited to cell phones, cameras, recorders and camera phones.

The Agency will maintain a privacy statement accessible off of the home page on the Agency web site.

11.2.3 Guidelines on Employee Use

Like all communications conducted on behalf of the State of Kansas, employees must use good judgment in Internet and e-mail use. Each use of the Internet and each e-mail must be able to withstand public scrutiny without embarrassment to the Agency or the State of Kansas.

Users are responsible for any and all activity initiated by their e-mail ID, user-id or personal workstation. Users shall archive their e-mail as appropriate in a central e-mail record archive.

Individuals must not disclose internal Agency information via the Internet or e-mail system that in any way adversely affects Agency customer relations or public image.

As mentioned in section 1.5 of this document, the Agency has issued an Acceptable Use Policy for Agency provided Information Technology Resources. This policy covers the use of the Internet and e-mail and is mandatory for all employees, agents, associates, representatives, interns, contractors, temporary employees, assignees, or other designees of the Agency.

11.3 Voice Mail Systems

Voice mail may be used to receive and retrieve messages when employees are unable to answer their telephone. This communications device is usually connected to the telephone switches through call routing via extensions and the potential for unauthorized message receiving or fraudulent calling can occur.

The following steps should be taken to minimize fraudulent use of voice mail:

- Never allow external incoming calls to be transferred to outside lines.
- Never use easy or obvious passwords and change them often.
- Delete unassigned mailboxes.
- Monitor activity logs for repeated login attempts to specific mailboxes or to repeated random login attempts.
- Lock the mailbox after 3 unsuccessful login attempts.
- Require users to create personal greetings and to change the default password when setting up their mailbox.
- When an employee leaves the Agency for another employer or agency, the immediate supervisor must notify the voice mail administrator at the Agency in order for the administrator to remove the departing employee from the voice mail system.

11.4 Remote Access

Dial-up access via a modem poses a high risk of possible intrusion to the Agency network. At the same time remote access conveniently enables Agency employees, contractors and vendors to access Agency computer resources from offsite locations.

Agency networked systems should not be accessed over the Internet using Agency assigned user ids unless passwords are encrypted. Other protected transmission means such as the dial-up facilities must be used instead.

The Agency should consider the use of automated software to ensure that any device connecting to the network has the current level of security patches and anti-virus installed. Otherwise the device should be quarantined and updated first.

The use of individual modems connected to single PCs, terminals, or servers provide unprotected “back doors” to the entire Agency network and must not be permitted without specific protective measures.

11.5 Video

Video conferencing capabilities are offered to the entire State through the KANSAN network. This service is being used for classroom training, meetings, and public hearings as well as confidential hearings. Following are requirements for video conferencing:

- No unauthorized recordings will be made of any videoconferences.
- There will be no unauthorized play back of authorized conference recordings.
- Operations center employees responsible for administering connections for video conferencing will not record, play back or listen in on conference calls unless they are instructed to do so by the hosting party of the video conference.

11.6 Virus Detection and Protection

Computers infected with viruses or malicious code could jeopardize information security by contaminating data. This policy provides controls to protect against such attacks. Please refer to Information Security Incident Reporting information in section 4 for appropriate action for detected or suspected viruses.

A typical virus is a small computer program that, as part of its operations, reproduces itself by making copies of itself and inserting these copies into uninfected programs or data files. This insertion process takes only a fraction of a second, a virtually undetectable delay. The infected program will subsequently execute the virus code during its normal processing. In addition to its ability to reproduce, the virus may cause damage to the programs, data, or equipment, or it may perform some other function that is relatively harmless. Viruses can use one or more technique to achieve their purpose. Sharing data files can spread them. Personal computing environments are more susceptible to viruses, however, they can occur in the mainframe-computing environment as well. The following are controls that can reduce the chance of virus infection within the personal computing environment.

	CONTROL NAME	CONTROL STANDARD
	Virus Detection Software	Virus detection or integrity checking software should be used in all PC/LAN environments, including portable PCs and PCs located at employees' homes.
	Updating Virus Detection Software	The data files used by the detection software must be updated regularly to ensure system scans can identify most known viruses. A program to monitor vulnerability lists must be Implemented on a regular basis.
	Loading Software	a) No unapproved software may be loaded on State of Kansas PCs or LANs. b) All software introduced into State of Kansas PC/LAN computing environments, including State of Kansas PCs that are located in employees' homes, must be known to be virus free. c) All PC/LAN computing environments into which State of Kansas software and/or data is introduced must be known to be virus free. d) Software distributed from any State of Kansas PC/LAN computing environment to another State of Kansas organization or a State of Kansas customer must be known to be virus free.
	Verifying software	Virus scans or integrity checks must be done prior to the first use of each executable file that is brought into the State of Kansas environment from un-trusted environments, e.g. program fixes copied from vendors' bulletin boards or web sites.
	Scanning Removable Media	Virus scans or integrity checks must be done prior to the first use of each diskette (or other removable media) after the diskette has been out of a State of Kansas-controlled environment. Examples: Diskettes used in a PC at home, whether owned by State of Kansas or not. Diskettes used in a customer or vendor's computer.
	Scanning Frequency	Virus scans of permanent media must be done at least daily: a) On any server connected to a network, e.g. a server connected to a LAN. b) On computers used for distribution of files outside of , e.g. those used to send files to external customers, user

		groups, or vendors c) On any workstation that shares software with any other computer. d) On computers running an application for which the risk is medium or high for loss of data or loss of the application. Virus scans must be done at least weekly in all other situations.
	Scheduling Virus Scans	Whenever possible virus scans should be scheduled to occur automatically. (All files should be scanned before being loaded on the network and a weekly network scan should be scheduled as well.)
	Audit Records	Records must be kept that show scans occurred and the details of any findings from the scans. Note: Some scanning software provides customized logs.

11.7 Wireless

.

With the advantages that Wireless technology brings to the State of Kansas, it also brings inherent security vulnerabilities. Wireless networks are attractive targets for all types of unauthorized access attempts. From casual users looking for free access to the Internet, to malicious intruders looking to gain unauthorized access to confidential information on Wireless clients and State owned applications, robust security mechanisms are needed to protect the information assets of the State.

To meet the security goals of confidentiality, integrity, and availability, agencies will follow the Information Technology Policy #7500- Wireless Local Area Network Policy.

Appendix A: Security Acknowledgement

The following is an example of an Employee Agreement that all State agencies should establish and maintain.

Employee Agreement to Comply With
(State Agency) Information Technology Security Policy

The State of Kansas is devoted to information security and employs specialists to maintain security. However, it is the responsibility of users to comply with all information security policies and procedures.

By signature below, the employee hereby acknowledges and agrees to the following:

1. Employee is a "user" as defined in the State of Kansas Information Technology Security Requirements

2. As a user, employee shall comply with security measures dictated by both "owners" and "custodians," as defined in the State of Kansas Information Technology Security Requirements

3. Employee is a State of Kansas employee in possession of State of Kansas information resources

4. Employee shall protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

5. Employee has read and agrees to abide by the "State of Kansas Information Technology Security Policy" manual.

6. Employee agrees to discuss with a supervisor regarding policies or procedures not understood.

7. Employee shall abide by the policies described as a condition of continued employment.

8. Employee understands that any employee found to violate these policies is subject to disciplinary action, including but not limited to, privilege revocation and/or termination of employment.

9. Access to State of Kansas information systems is a privilege, which may be changed or revoked at the discretion of management.

10. Access to State of Kansas information systems automatically terminates upon departure from the State of Kansas employment.

11. Employee shall promptly report violations of these policies to the appropriate agency security office.

12. This document may be amended from time to time. The State of Kansas will notify employees of amendments. Employee will keep abreast of amendments to the "State of Kansas Information Technology Security Requirements," as made available by hard copy or on-line.

ACKNOWLEDGMENT: STATE OF KANSAS INFORMATION TECHNOLOGY POLICY

_____ _____

User's signature Date Witness Date

_____

User's name in block capital letters

Appendix B: Web-Enabled Application Security Policies

Introduction

As existing mainframe applications are web-enabled, or new web applications are built, appropriate information security and audit controls must be incorporated into them. Because the Internet is designed for open interconnectivity, many security concerns arise. The application developer, working in conjunction with the application owner, must address these concerns. The application owner has the ultimate responsibility for ensuring the appropriate levels of security and control.

Security Implications for System Development and Testing

In general, the following security aspects must be considered during system development and testing of any application or when new application systems are acquired:

- Determine the sensitivity and criticality of the system information.
- Assess the threats and vulnerabilities that exist relative to the system assets.
- Identify security alternatives and basic security framework in the selected system architecture.
- Identify organizational vulnerabilities that could result from a significant breach of security.
- Define security requirements and select the appropriate controls.
- Include approved security requirements and specifications in the development baselines.
- Develop security test plans.
- Conduct tests of security in the configured components and in the integrated system.
- Prepare documentation of security controls and safeguard it.
- Conduct acceptance test and evaluation of system security.

Requirements for Web-Based Applications

More specifically, when applications are web-enabled the following basic security must be addressed:

- Authorization- ensuring authorized uses of systems and performance of business function by authorized users only.
- Authentication- establishing that parties to an electronic transaction or communication are who they claim they are.
- Integrity- ensuring that data on the host system or in transmission are not created, intercepted, modified, or deleted illicitly.
- Confidentiality- warranting that data is only revealed to parties who have a legitimate need to know it or have access to it.
- Availability- ensuring that legitimate access to information and services is provided.
- Non-repudiation- if a party to some transaction or communication later denies that it has ever happened, some mechanism is in place to facilitate dispute resolution.
- Privacy- ensuring that customer's personal data collected from their electronic transactions is protected from unauthorized disclosure.

Overall System of Security

The above requirements should be considered under the context of an overall system of security. For an effective security system, many categories of security must be considered and harmonized into an overall plan. Omission of any one of these categories creates a hole through which the overall system can be compromised.

The categories are as follows:

Physical Security involves the security of the physical devices, which includes the ability to control access to such hardware. Application developers and owners should:

- Ensure that all Desktop Equipment, Servers, Data Centers, Telecommunication Rooms, Wiring Closets, Offsite Storage, and Alternative Work Sites are appropriately secured and controls are in place to restrict the access/entry of personnel to only authorized individuals.
- Locate all equipment in environmentally appropriate facilities and utilize environmental controls such as water detection, smoke detection, fire prevention, and uninterruptible power supplies.
- Provide Intrusion detection systems that signal an alarm when unauthorized entry is attempted.

User Security addresses the ability to ensure that the user accessing data and systems is in fact who they say they are and that they have access only to those resources to which they are authorized. Functions that are involved in this issue include identification, authentication, and authorization of the individual, as well as non-repudiation and audit. Application developers and owners should:

- Address the Identification function by utilizing some method of ensuring that only authorized individual users are permitted access to information systems. The user must be required to provide some unique identification (e.g. User ID), to provide a claimed identity to the system. These means of identification should be administered by an appropriate source, independent of the users and inactive User Ids should be removed in a timely manner. (Refer to specific user id rules)
- Address the Authentication function by validating a user's claim to who he/she is. This should be based on something the individual knows (e.g. a password), something the individual possesses (e.g. a smart card), or by something the individual is, (a biometric). Responsible password management should be employed whenever authentication is based on passwords (e.g. Password aging, minimum length, mixed characters, etc). (Refer to specific password rules)
- Address the non-repudiation requirement by utilizing Public Key Infrastructure (PKI) technology to provide the assurance that the information received has not been altered and also that the reputed sender of the information is indeed who sent it.
- Address the Authorization function by determining the appropriate levels of access for all users for all systems, based on need to know, specific job responsibilities, and sensitivity of the data. Directory-based services or LDAP can be used.
- Address the Audit function by maintaining automated records to enable reconstruction and/or review of operations performed on systems. Audit trails should be protected in such a way that a user can not change them. They should be reviewed regularly by individuals in a supervisory or security capacity.
-

Application Security concerns the built-in security features of the application itself. Application developers and owners should:

- Ensure that the security features of the application code are consistent with the overall security policies enumerated in this document.
- Document all interfaces between applications and explain how the components will securely communicate with one another.
- Document the use of all middleware, which is software that connects two otherwise separate applications. An example is software that connects the web server to the database server.

System Security involves the analysis of the overall operating systems and software used to support the applications software. Whether the operating system is mainframe, server or PC based, or a combination thereof, Application developers and owners should:

- Ensure that research is done for known security vulnerabilities.
- Install vendor-supplied security upgrades and patches.
- Remove or disable any service not required.
- Acquire additional security software as needed to reside on the system.
- Consider vulnerability scans to pinpoint the weaknesses of the system.
- Install intrusion detection systems and monitor them for unauthorized access.

Data Security encompasses both physically protecting the application data from unauthorized access as well as loss of data through mechanical/electrical failure or viruses. Application developers and owners should:

- Utilize at least 128-bit encryption for any data transmitted over public networks.
- Ensure that all FTP transmission of data over insecure channels is encrypted.
- Require that Authentication is used at all times when accessing or making changes to data.
- Ensure that Auditing is activated and all access to data is logged.
- Determine the Backup and Archive procedures that will be used.
- Determine the Off-site storage requirements of backups and archives.
- Consider the encryption of backups when highly sensitive data is involved.
- Specify what virus control software and detection procedures will be used to protect the data.

Network Security includes the physical/electrical links between the Desktop Client and the Host computer. The responsibility for Network Security is generally split between Agencies, with the User Agency and DISC performing part of the functions. In view of this, close cooperation between these groups must be maintained. Application developers and owners should:

- Document the network environment with a diagram that shows all links and component parts.
- Ensure that the LAN is isolated from any network-connected device that does not have a valid business relationship with resources on the LAN.
- Place a firewall between the LAN and the Internet to prevent untrusted networks from accessing the Agency LAN. Public access should never be allowed into the secured private LAN.
- Recognize that if public access to a server in the internal LAN is required, it is best to put that server on a separate LAN segment behind the firewall device typically referred to as the DMZ.

Security Administration involves the administration of the overall security plan. Application developers and owners should determine who will have specific responsibility and what policies and procedures they will employ for the following:

- authentication (read, write, modify, delete) services to provide users with user ids and passwords
- authorization (read, write, modify, delete) services to provide users access to applications
- generation and distribution of reports for monitoring access and potential security breaches. Reporting and monitoring activity should include reports based either on the individual initiating the event or the data and resources affected by the event. These reports should be distributed on a regular basis to the data owners. Reports can include: attempted or actual access violations for data and resources, invalid logon attempts, access trends and deviations from those trends, access to sensitive data and resources, access to data or resources by privileged users, or, access modifications made by security personnel.

- Developing an incident handling procedure.
- the periodic testing of the existing security plans, including both Business Recover Plans and protection against unauthorized intrusion.

Social Engineering/Human Factors are concerned with the techniques that employ the use of deceptive practices aimed at individual users or employees. All computer networks and applications are susceptible to compromise by malicious or unauthorized persons. Application developers and owners should:

- Make staff members at all levels aware of the potential to be used as a resource to enable illegitimate access to systems or network infrastructure.
- Instruct all employees or users of the application to exercise caution to prevent the release of sensitive details to unauthorized sources.
- Prohibit the release of passwords via telephone or unsecured electronic mail.
- Maintain a list of technical support authorized to request information.
- Encourage users to have vendors, outside technical support or contractors contact the organization's IT staff support for information pertaining to the network or information access.

Appendix C: Requirements for Use of Federal Tax Information from the IRS

An Agency that receives Federal Tax Information (FTI) from the IRS must safeguard the FTI in accordance with IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies.* The requirements are as follows:

Record Keeping for Electronic Files

Authorized employees must be responsible for securing magnetic media before, during, and after processing and ensuring that the proper acknowledgement form is signed and returned to the IRS.

Inventory records must be maintained for purposes of control and accountability.

Media containing FTI, any hard copy printout, or any file resulting from the processing of such media will be recorded in a log that identifies:

- Date received
- Media control number
- Number of records if available
- Movement and
- If disposed of, the date and method of disposition.

Semiannual magnetic media inventories will be conducted.

Secure Storage

Care must be taken to deny access to areas containing FTI during duty hours. This can be accomplished by restricted areas, security rooms, or locked rooms. In addition FTI in any form (computer printout, photocopies, tapes, etc.) must be protected during non-duty hours. This can be done through a combination of methods: secured or locked perimeter secured area or containerization.

Restricting Access

Access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated.

If FTI is recorded on magnetic media with other data, it should be protected as if it were entirely FTI.

The two acceptable methods of transmitting FTI electronically over telecommunications devices are encryption and the use of guided media (which involves the use of protected microwave transmissions or the use of end to end fiber optics).

All computer systems processing, storing, and transmitting FTI must have computer access protection controls at Level C2 as covered in the next section.

Computer Security

All automated information systems and networks that process, store, or transmit sensitive but unclassified information, such as FTI, must meet the requirements for Controlled Access Protection (Level C2) as evaluated by the National Institute of Standards and Technology.

To meet C2 requirements, there are “fourteen major points” or areas that must be addressed. There are also three tiers of Systems to be evaluated:

- Tier I- Mainframe and Microprocessor Systems
- Tier II- LANS,WANS, File Servers, etc
- Tier III- Personal Computers, Laptops, Workstations

Not all of the points are necessarily applicable to all of the Tiers. The fourteen points are as follows:

- Discretionary Access Control (DAC) - A means of restricting access to objects based on the identity and need-to-know of the users and/or groups to which they belong.
- Object Reuse - A means of preventing unauthorized access by clearing all protected information on objects before they are allocated or reallocated out of or into the system. If an object, such as a disk, tape or storage devices which may be used for printing, file servers, etc., is to be taken out of a system and made available for other uses, it must be cleared of all protected information. This does not include tapes/disks, which are used to store data for reuse in the same program or tapes/disks, which are specifically assigned to a single program, and to which only individuals with the same authorizations and need-to-know have access to the data. Objects being allocated into the system also must not contain residual protected data, which other users may access.
- Identification - Identification ensures individual accountability through identification of each individual system user. Identification is often accomplished with login Ids or user Ids. All Ids must be unique and auditable.
- Authentication - Authentication is the process that ensures individual accountability through the validation of each individual system user. It is often accomplished with passwords.
- Audit - Audit requires the maintenance of an audit trail of accesses to the objects and data it protects. The audit trail is a systemic record that is sufficient to enable reconstruction and/or review of activities related to operations, procedures, or events occurring on that system. Audit trails must, at a minimum, be able to record log-in attempts, password changes, and file creations, changes and/or deletions. The audit trail must be protected in such a way that it can not be changed by the user. Audit trails must be reviewed regularly by supervisory, security, or other authorized agency individuals who are not the regular program users.
- System Architecture - System Architecture insures that the Trusted Computing Base (TCB) maintains a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures).
- System Integrity - System Integrity requires that hardware and/or software features will be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.
- Security Testing - Security Testing requires that the security mechanisms of the computer system are tested and found to work as claimed in the system documentation. Testing shall be found to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.
- Security Features User’s Guide - A single summary, chapter or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.
- Trusted Facility Manual - This is a manual addressed to computer system administrators, and will present cautions about functions and privileges that should be defined and controlled when running a secure facility.

- Test Documentation - This document describes the test plan, test procedures that show how the security mechanisms were tested and results of the security mechanism's functional testing.
- Design Documentation - This provides a description of the manufacturer's philosophy of protection and an explanation of how the philosophy is translated into the TCB.
- Communications Infrastructure - The communications specialists shall ensure that this infrastructure is afforded the same security as other hardware associated with the system to be protected. Intrusion detection devices, line monitoring devices, firmware utilities, and other software solutions should be incorporated into this security requirement to ensure that when authorized users access system resources, their transmissions are protected from unauthorized access by others. Documentation defining connectivity should be maintained and updated regularly, including data system specifications, wiring configurations, system connectivity, and remote access documents.
- Encryption Methodology - This defines how data objects are altered (ciphered), so that they become unreadable until deciphered. This methodology can be applied directly to the data objects, or to the communications platform that supports the inter-connectivity between systems that process, store and transmit IRS tax data.

Other Safeguards

Before granting employees access to FTI, employees must read the Agency Confidentiality Agreement and sign the Agency Confidentiality Oath. This document includes the FTI Confidentiality Provisions from the Internal Revenue Code and the penalties that apply for improper actions.

On at least annual intervals, employees should be reminded of the provisions of the Confidentiality Policy.

The Internal Audit unit or Agency Head designee shall perform independent Internal Inspections to ensure that adequate safeguard and security measures have been maintained. Inspection reports, including a record of corrective actions, shall be maintained for a minimum of three years from the date the inspection was completed. A summary of the inspection reports shall be included with the annual Safeguard Activity Report submitted to the IRS.

Any statistical reports containing FTI will be done in a form such that the identity of particular taxpayers can not be identified, either directly or indirectly according to the provisions of Publication 1075.

Reporting Requirements

The Agency Federal State Coordinator will submit to the IRS a Safeguard Procedures Report every six years or whenever significant changes occur in their safeguard program as prescribed in Publication 1075. This report is a record of how FTI is processed and safeguarded by Agency.

The Agency Federal State Coordinator will submit to the IRS a Safeguard Activity Report annually as prescribed in Publication 1075. This report includes changes to the information or procedures previously reported, current annual period safeguard activities, actions on Safeguard Review recommendations, and planned actions affecting safeguard procedures.

Disposal of FTI upon completion of use

When finished with the use of FTI, the Agency will ensure the following occurs:

- Either return the information to the IRS office that it was originally obtained from or make the information "undisclosable" and include in the annual report to the IRS a description of the procedures used.
- When paper documents containing FTI are to be destroyed, they will be shredded using an IRS approved shredder.
- When magnetic tapes or cartridges containing FTI are to be destroyed, they will be degaussed using IRS approved equipment.
- When disk media containing FTI is to be destroyed, it will either be degaussed or damaged in an obvious manner to prevent use and discarded.

Disclosure to Contractors

Agency will observe the following requirements:

- Disclosure of FTI is generally prohibited unless authorized by statute.
- For authorized disclosures, Agency will notify the IRS prior to the execution of any agreement to disclose to a contractor, but in no event less than 45 days prior to the disclosure of FTI.
- Agency will ensure that all employees of the contractor have signed the Agency Confidentiality Agreement.
- Agency will include the appropriate safeguard language as contained in Exhibit 5 of Publication 1075 in all contracts.

Appendix D: Stages of Responding to an Incident

There are six identifiable stages of response to an information security incident:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up.

1. Preparation
One of the most critical facets of responding to incidents is being prepared to respond *before* an incident occurs. Part of the preparation has been to install a baseline of protection on all systems and networks. All computing components should have at least a minimum level of defense if not, incidents can spread very quickly from system-to-system
Plan Communications. The tendency for the unexpected to occur during incidents often adversely affects ability to communicate with others. Contact lists with duty and home phone numbers of personnel to be contacted during incidents should be prepared and widely distributed. Issuing pagers to key personnel is also a wise step in preparing for incidents.

Establish firecall procedures. Firecall procedures are procedures to provide operational continuity when there is a significant risk of prolonged failure or disruption. Assigned system administrators may not be available during a critical incident involving one or more of the systems. Ensure, therefore, that the passwords used to obtain superuser access to every system and LAN within your organization are recorded on a sheet of paper, sealed in a signed envelope, and placed in a locked container in case superuser access is needed by someone other than the assigned system administrator. Storing encryption keys for critical information in this manner is also advisable. Firecall procedures must include provisions for verifying the identity of the person who needs a password or encryption key during an emergency.

Regularly backing up systems and data helps ensure operational continuity. This practice also enables personnel to check the integrity of systems and data and to verify whether unauthorized changes have occurred by comparing files to their corresponding backups. Because recovery is often a complex process, establishing and following recovery procedures is also a critical part of the preparation process. Standardizing these procedures makes it easier for *anyone* to perform them during an emergency someone not assigned to a particular system or network may be called on to perform recovery procedures.

2. Identification
Identification involves determining whether or not an incident has occurred, and if one has what the nature of the incident is. Identification normally begins after someone has noticed an anomaly in a system or network. Determining whether or not that anomaly is symptomatic of an incident is often difficult. Anomalies often turn out to be benign evens such as errors in OS or application configuration, hardware failures, and, most commonly, user errors. The written procedures recommend trained personnel to accomplish this step.

Backup. It is extremely important to obtain a full image backup of the system in which suspicious events have been observed as soon as the possibility that a security-related incident has occurred is indicated. Perpetrators of computer crime are becoming increasingly proficient in quickly destroying evidence of their illegal activity. Unless this evidence is immediately captured by making a full backup, this evidence may be destroyed before you and others have a chance to look at it. The backup will, in addition provide a basis for comparison later in case you need to determine if any additional unauthorized activity has occurred. Be sure to safely store any backup tapes so that they will not be lost and/or stolen.

Record Keeping. Ensure a logbook is used to record the nature of suspicious events observed immediately after they've been observed. Include the name of the system, time and other details related to the observations (even though they may not seem to be very relevant at the time they are recorded). Also record the names of those with whom the incident or possible incident was discussed. Careful recording of these details can assist efforts to identify the nature of an incident, develop effective solutions, and prosecute those who commit computer crime. Be sure additionally to safely store the logbook. Software packages can be helpful in identifying incidents. Virus detection packages are useful in detecting viruses. Intrusion detection tools can indicate whether someone has broken into a account on a system or has misused the system. System and network audit logs also generally provide sufficient information to facilitate deciding whether or not unauthorized activity has occurred.

3. Containment

Containment, the third stage of responding to incidents, involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve using malicious code, incidents can spread rapidly, causing massive destruction and compromise of information. It is not uncommon to find that every unprotected workstation connected to a LAN is infected when there is a virus outbreak. As soon is suspected, immediately begin working on containing the incident.

The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. Work within your chain of command to determine whether sensitive information (and in the case of classified systems, classified information) should be left on information systems or whether it should be copied to media and taken off-line. It may similarly be best to move critical computing services to another system on another network where there is considerably less chance of interruption.

The next decision concerns the operational status of the compromised system itself. Should this system be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that any activity on the system can be monitored? The answer depends on the type and magnitude of the incident. In the case of a simple virus incident, it is almost certainly best to quickly eradicate any viruses without shutting the infected system down. If the system is classified or sensitive, information or critical programs may be at risk, and it is generally best to shut the system down (or at least temporarily disconnect it from the network). If there is a reasonable chance that a perpetrator can be identified by letting a system continue to run as normal, risking some damage, disruption, or compromise of data may be advisable. Again, work within your chain of command to reach a decision.

4. Eradication

Eradicating an incident entails removing the cause of the incident. In the case of a virus incident, eradication simply requires removing the virus from all systems and media (e.g., floppy disks), usually by using virus eradication software. In the case of a network intrusion, eradication is more ambiguous. Bringing the perpetrators into legal custody and convicting them in a court of law best eradicate network intrusions. From a statistical viewpoint, however, the likelihood of obtaining a conviction is very small. The network intruder(s) may instead simply terminate efforts to gain unauthorized access or may temporarily terminate an attack, then attack the same system again several months later.

5. Recovery

Recovery means restoring a system to its normal mission status. In the case of relatively simple incidents (such as attempted but unsuccessful intrusions into systems), recovery requires only assurance that the incident did not in any way affect system software or data stored on the system. In the case of complex incidents, such as malicious code planted by insiders, recovery may require a complete restore operation from backups. In this case it is essential to first determine the integrity of the backup itself. Once the restore has been performed, it is also essential to verify that the restore operation was successful and that the system is back to its normal condition.

6. Follow-up

Some incidents require considerable time and effort. It is little wonder, then, that once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in responding to incidents. Following up afterwards helps organizations improve their incident handling procedures as well as continue to support any efforts to prosecute those who have broken the law. This final step should include a detailed analysis of the event should address the following

- What has transpired and what was done to intervene?
- Was there sufficient preparation for the incident?
- Did detection occur promptly or, if not, why not?
- Could additional tools have helped the detection and eradication process?
- Was the incident sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?
- What was the cost (personnel time, downtime, cost of loss of productivity, etc)?
- How much did the incident disrupt ongoing operation?
- Was any data irrevocably lost? If so, what was its value?
- Was any hardware damaged?

Appendix E: Web-enabled Security Questionnaire

Physical Security involves the security of the physical devices, which includes the ability to control access to such hardware—

1. What are the various hardware devices envisioned to be used, and at what locations?
2. Who will have access to the various physical components and how will access be controlled?
3. Are environmental controls adequate for smoke, water detection and fire prevention?
4. What Uninterruptable Power Supply (UPS) will be used and what characteristics will it have?

User security addresses the ability to ensure that the user accessing data and systems is in fact who they say they are and that they have access only to those resources to which they are authorized. Functions that are involved in this issue include identification, authentication and authorization of the individual, as well as non-repudiation and audit

1. How will users be identified to the systems
2. What unique form of identification will be used (Userid)?
3. Who will administer the Userids?
4. What provision is made to remove inactive users, by whom and how timely?
5. How are users authenticated into the system (passwords, smartcards, biometrics)?
6. Where passwords are used, what are the specific password rules (minimum length, character makeup, aging etc.)?
7. How is assurance provided that the information received has not been altered?
8. How is assurance provided that the reputed sender is indeed the one who sent it?
9. What levels of system access are there?
10. Who determines and maintains system access?
11. What provisions are made for audit trails to enable reconstruction and/or review of operations performed on the system?
12. How are audit trails protected from unauthorized changes?
13. How often will system logs be reviewed and by whom?

Application Security concerns the built-in security features of the applications involved

1. Describe what security features are built into the various system applications.
2. How specifically do these security features work?
3. If these applications communicate to other systems, how is this accomplished? (e.g. web server to database server).
4. Has autocomplete been disabled for all input fields on applications using Microsoft Internet Explorer 5.0 or above?
5. What information is logged for each transaction? (The minimum is Userid, IP address, and time and date stamp)
6. What provision is made for time synchronization to enable accurate logging?
7. Where will logging information be stored?
8. Do applications use session tokens that are custom created or default from a vendor, (e.g. Microsoft)?
9. Does the application store any cookies on client machines? If so, what are they?
10. Are cookies checked for validity when returned back to servers?
11. Are sessions and/or cookies destroyed when the user logs out of the application?
12. Does the application require re-authentication for critical user actions such as money transfer?
13. What security controls are built around files where Userids, passwords, Pins, etc are stored?
14. Are all authentication events (logging in, logging out, failed logins, etc) logged?
15. Are all administrative events (account management actions, enabling or disabling logging etc.) logged?
16. Are logs written so only new records can be added, and existing records not overwritten or deleted?
17. What client-side data validation is to be performed?
18. What data validation is to be performed on the server side? How will this be performed?
19. How is editing done to prohibit generic meta-characters from being present in input data?
20. Are all database queries constructed with parameterized stored procedures to prevent SQL injection?

21. Can any variables be used in script? If yes, how are they protected to prevent direct operating system command attacks?
22. What scripting language is to be used? Has this language been checked for vulnerabilities and have they been addressed?
23. Does the application do security checking after UTF-8 decoding is completed?
24. Will all comments be removed from any code that could be passed to the browser?
25. Will users be able to see any debugging information on the client?
26. Will all sample, test, and unused files be removed from the system?
27. Will pages with personal data be cached?
28. Will forms submissions be done using a POST request as opposed to a GET?

System Security involves the analysis of the overall operating systems and software used to support the applications software

1. What research has been conducted for known security vulnerabilities? What are the results of that research?
2. Who will install vendor-supplied security upgrades and patches?
3. How will timely installation of patches and upgrades be accomplished?
4. Will unnecessary services be disabled? Which ones?
5. Will debugging mode on web server(s) be disabled in production?
6. Will default accounts be disabled and passwords changed from defaults?
7. Will the database user have limited abilities in being only able to run stored procedures or select?
8. Will you have formal server hardening procedures?
9. Will you have formal desktop/laptop hardening procedures?

Data Security encompasses both physically protecting the application data from unauthorized access as well as loss of data through mechanical/electrical failure, viruses or hacking.

1. Will authentication used at all times when accessing or making changes to data to ensure confidentiality
2. Will at least 128-bit encryption be used for any data transmitted over public networks?
3. Will databases be encrypted?
4. Will all FTP transmissions of data over insecure channels be encrypted using PGP software?
5. Will auditing be activated and all access to data be logged?
6. What are the backup and archive procedures that will be used?
7. What are the offsite storage requirements envisioned for backups and archives?
8. Will backups be encrypted if sensitive data is involved?
9. What virus control software and detection procedures will be used to protect data?
10. How will privacy be maintained to ensure that customer's personal data collected from electronic transmissions is protected from unauthorized disclosure?

Network Security includes physical/electrical links between desktop/laptop client and host

1. Provide documents to show the network environment diagram showing all links and component parts.
2. As above, show all connections to the Kansas IT network (KANWIN)
3. Describe provisions for automated anti-virus protection for each device in this application that connects to KANWIN
4. How will the LAN be isolated from any network-connected device that does not have a valid business relationship with resources on the LAN?
5. Are firewalls used between the LAN and the Internet to prevent untrusted networks from accessing the LAN?
6. If public access to a server in the internal LAN is required, will the server be put on a separate LAN segment behind the firewall device typically referred to as the DMZ?
7. Will intrusion detection/intrusion prevention devices be utilized?
8. How will intrusion devices be monitored and over what duration?

Security Administration involves the administration of the overall security plan

1. Who will be the security administrators for the application?
2. What functions will they provide?
3. How will users be provided with Userids and passwords?
4. Will passwords be restricted from being distributed via telephone or unsecured electronic mail?
5. How will unusual security incidents be handled?
6. Will employees or users of the application be instructed on how to handle and prevent the release of sensitive information?

Appendix F: References

The National Electronic Commerce Coordinating Council, Identity Management, December 2002

Information Technology – Security Techniques – Code of Practice for Information Security Management, ISO/IEC 17799-2005(E)

National Institute of Standards and Technology, Risk Management Guide for Information Technology Systems, 800-30, July 2002

Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments, Carnegie Mellon University, CMU/SEI-2005-TN-032

The Internet Revolution Cool Tool. Useful Tool. Life Tool, RSA Security, INTR WP 0504, 2004

Kansas Administrative Regulations, 2005

Kansas Certificate Policy, ITEC, 2004